

(12) UK Patent Application (19) GB (11) 2 267 984 A (13)  
(43) Date of A publication 22.12.1993

(21) Application No 9212796.8

(22) Date of filing 16.06.1992

(71) Applicant  
Thorn EMI Electronics Limited  
(Incorporated in the United Kingdom)

Jubilee House, 120 Blyth Road, Hayes, Middlesex,  
UB3 1DL, United Kingdom

(72) Inventor  
Richard Cedric D'Agnall Clutterbuck

(74) Agent and/or Address for Service  
David E Osborne  
Thorn EMI Patents Limited,  
Central Research Laboratories, Dawley Road, Hayes,  
Middlesex, UB3 1HH, United Kingdom

(51) INT CL<sup>6</sup>  
G06F 13/40 13/372

(52) UK CL (Edition L)  
G4A AFGT  
G4Q QBW

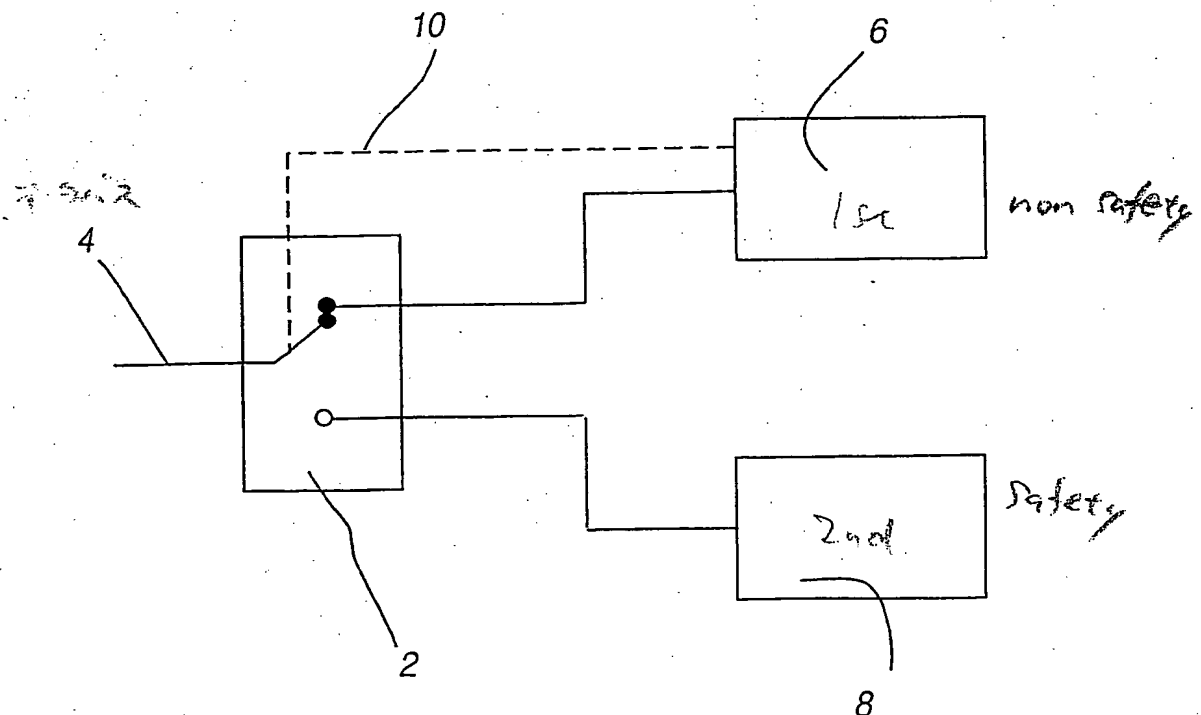
(56) Documents cited  
GB 2162975 A

(58) Field of search  
UK CL (Edition K) G4A AFGK AFGT  
INT CL<sup>5</sup> G06F 13/372 13/40

(54) Multiplexing bus interface

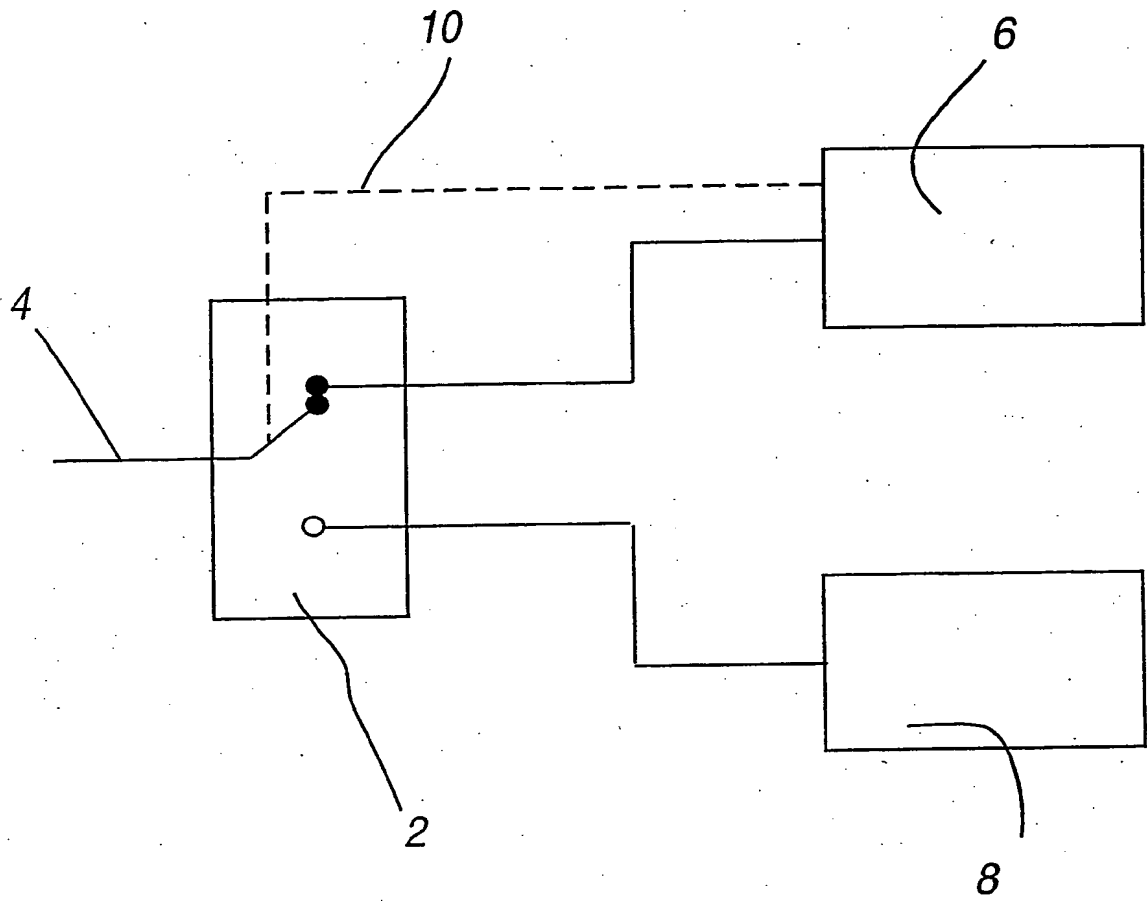
(57) A bus interface (2) couples either a first portion (6) or a second portion (8) to a data bus (4). The state of the interface is controlled by the first portion, such that the second portion is only coupled to the data bus for predetermined periods.

The apparatus is particularly suitable for use in systems having safety-critical functions, since it enables non-safety-critical functions of the system to be controlled by the first portion (6) and be re-programmable, whereas the second portion (8), which would not be re-programmable, may control safety-critical functions of the system.



This print incorporates corrections made under Section 117(1) of the Patents Act 1977.

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.



DATA PROCESSING APPARATUS

This invention relates to a data processing apparatus, and more particularly to such an apparatus which may be used in a system having safety critical functions.

There are many instances of systems having both safety-critical and non safety-critical functions, such as traffic control or plant control systems. For example, in railway signalling systems, safety-critical functions include those which prevent danger to people or material, such as the control of signals for ensuring safe positioning of rolling stock. However, functions which relate to the train number or timing are not safety-critical so that, for example, a particular train may depart at a time which differs from that of the time-table without affecting safety.

In designing such systems having safety-critical aspects, considerable care must be taken to ensure that a failure in any component of the system cannot endanger the safety of the system.

Integrated circuits therefore undergo failure modes and effects analyses to ensure that any failures possible do not compromise the system, and programming associated with computers must be rigorously analysed to ensure that any errors in the input, or in the storage of the programme itself, cannot cause failures of the safety-critical aspects of the system.

Re-programmable computer systems are not normally suitable since it is possible that a new programme could be introduced that bypasses existing interlocks, and causes safety-related failures. These changes could be introduced deliberately, or by bit change errors in the computer memory which, since it is designed to be re-programmable, will be more susceptible to such changes than a non re-programmable memory system.

In the past, these constraints have led to safety systems being designed using custom ASICs, and other non programmable hardware. The increasing complexity and flexibility of modern

safety systems, however, means that the special integrated circuits designed for these systems are becoming increasingly complex, and from an engineering viewpoint could be better implemented in a computer-like system.

5        Attempts have been made to produce a re-programmable apparatus for use in a system having safety-critical functions, which apparatus includes two components, namely a re-programmable computer component and a non-re-programmable safety-critical component. If the data is transmitted by a  
10 single medium, then to prevent confusion one of the components must have control over the data train. It is unsafe for the computer component to receive the data and send safety-related information to the safety-critical component, since it is possible that the computer will be re-programmed and send  
15 erroneous data to the safety-critical component, whilst replying to the data train to the effect that correct data has been transferred.

Conversely, the safety-critical component may receive the data, and send non-safety-related information to the computer  
20 component. The apparatus can be designed so that it is not possible for the computer to affect data in the safety-critical component, giving an apparatus which is both programmable and safe.

However, the safety-critical component must be designed to  
25 'understand' and correctly respond when connected to the data transmission system. Where the data transmission system is inherently simple, this results in little overhead in hardware terms. But many safety-critical components are now required to be connected to complex data transmission systems, on which the  
30 protocol of transmission would result in considerable design overheads to the safety-critical component. This is undesirable, since it is a fundamental tenet of safety-critical component design that the component should be as simple as possible.

35        Past designs of safety-critical components have used simple data transmission systems to avoid this difficulty, but with the

advent of requirements for interoperability, emphasis is now placed on the use of standard data transmission systems which, because of their required usage, must of necessity be more complex and capable than those systems used in the past.

5        Thus, if a complex data transmission system is required, with a computer in the safety-critical component capable of understanding the protocol used, it has been conventional to deny re-programmability of the computer.

10       It is an object of this invention to alleviate the problems outlined above.

      According to the present invention, there is provided data processing apparatus having a first portion and a second portion each being capable of being coupled to a data bus via an interface, the interface having a first state in which the first  
15       portion is coupled to the data bus whilst the second portion is not, and a second state in which the second portion is connected to the data bus whilst the first portion is not, the first portion being arranged to switch the interface from the first state to the second state for a predetermined time interval  
20       during which data destined for the second portion is being transmitted, and then to switch the interface back to the first state.

      The apparatus is particularly suitable for use in systems having safety-critical functions. In such a system, the first  
25       portion may control the non safety-critical functions of the system, whilst the second portion may control the safety-critical functions. The first portion is advantageously re-programmable by means of the data bus, the second portion not being re-programmable, enabling non-safety-critical functions of  
30       the system to be re-programmed, without any chance of a new programme affecting the safety-critical aspects, since the first and second portions cannot communicate with each other.

      Preferably, the first and second portions include first and second interfaces respectively, each being capable of being  
35       coupled to the data bus via a bus interface. The bus interface may be capable of determining the clock rate of the incoming or

outgoing data, and making it available to the first and second interfaces simultaneously. This allows the first portion to determine the time period for which the data bus should be connected to the second portion rather than to itself, and to  
5 control the bus interface accordingly.

The data destined for the second portion, which may be safety-critical data, is advantageously encoded, for example by a cyclic code having at least twenty parity bits. In this manner, if random data is transmitted to the second portion, for  
10 example due to the first portion erroneously connecting the data bus to the second portion, it is extremely unlikely that it could be observed as valid by the second portion. The second portion may alternatively be provided with other means for confirming correct reception of data.

15 In order that the invention may be more readily understood, reference will now be made, by way of example, to the accompanying drawing, which is a diagram showing data processing apparatus in accordance with the invention.

Referring to the drawing, a data processing apparatus for  
20 use in a system having safety-critical functions, such as a railway signalling system, comprises a bus interface 2 connected to a data bus 4 for transmitting and receiving data. The bus interface 2 is switchable between first and second states. In the first state, it connects the data bus 4 to a re-programmable  
25 first portion 6 for controlling non safety-critical functions of the system, and in the second state it couples the data bus 4 to a non re-programmable second portion 8 for controlling safety-critical functions. The coupling is achieved via first and second internal data interfaces respectively. The bus interface  
30 is controlled by the first portion 6 (as indicated by broken line 10).

In operation, the first portion 6 monitors the data being transmitted on the data bus 4. On receipt of appropriate codes, determined by the data transmission protocol, the first  
35 portion 6 may transmit and receive data applicable to itself and relating to non safety-critical aspects of the system.

The programming of the first portion 6 enables it to determine the position in the data train of safety-critical data destined for the second portion 8, such that it will operate the bus interface 2 for these time intervals only to connect the second portion 8 to the data bus 4. For example, the incoming data may be arranged to conform to a predetermined format in which a succession of synchronization words are each followed by a time frame, a first predetermined portion of which always contains data for the first component and a second predetermined portion of which always contains data for the second component. In such a case the first component may be programmed to recognise the arrival of each synchronizing word and switch the interface to the second component for the duration of the second predetermined portion of the immediately-following time frame.

If the programming of the first portion 6 is affected by errors, it will be unable to communicate. This fact may readily be detected, and the system caused to fail safe, the first portion 6 being unable to affect the second portion 8 directly.

The safety-critical data is encrypted in such a manner that the possibility of random data being decrypted in the safety system as valid data is extremely unlikely. Thus if the first portion 6 connects the data bus 4 to the second portion 8 at an inappropriate time, the probability of the second portion being wrongly programmed is negligible. For example, the safety-critical data can be transmitted encoded by a cyclic code with 20 or more parity bits. With suitable coding, this would provide less than one in  $10^{-6}$  probability that random data would be observed as valid. Cyclic coding is a relatively simple hardware function, and therefore adds little to the simplicity of the safety-critical second portion.

This invention therefore separates both the data and the hardware, such that it becomes possible to have a re-programmable computer placed in control of major functions and data transmission capabilities of the system, whilst retaining safety and allowing the safety system to communicate on the data bus.

CLAIMS

1. Data processing apparatus having a first portion and a second portion each being capable of being coupled to a data bus via an interface, the interface having a first state in which the first portion is coupled to the data bus whilst the second  
5 portion is not, and a second state in which the second portion is connected to the data bus whilst the first portion is not, the first portion being arranged to switch the interface from the first state to the second state for a predetermined time interval during which data destined for the second portion is  
10 being transmitted, and then to switch the interface back to the first state.
2. Data processing apparatus as claimed in claim 1, wherein the first portion is reprogrammable by means of the data bus whilst the second portion is not reprogrammable by means of the  
15 data bus.
3. Data processing apparatus as claimed in claims 1 or 2, wherein the interface is capable of determining the clock rate of data on the data bus, and making the clock rate available to the first and second portions simultaneously.
- 20 4. Data processing apparatus as claimed in any one of the preceding claims, wherein the data destined for the second portion is encoded.
5. Data processing apparatus as claimed in claim 4, wherein the data destined for the second portion is encoded by a cyclic  
25 code having at least twenty parity bits.
6. Data processing apparatus substantially as described herein, with reference to the drawing.

-7-

**Patents Act 1977**  
**Examiner's report to the Comptroller under**  
**Section 17 (The Search Report)**

Application number

GB 9212796.8

**Relevant Technical fields**

- (i) UK Cl (Edition K) G4A (AFGK, AFGT)
- (ii) Int Cl (Edition 5) G06F (13/40, 13/372)

**Search Examiner**

S J PROBERT

**Databases (see over)**

(i) UK Patent Office

(ii)

**Date of Search**

10 NOVEMBER 1992

Documents considered relevant following a search in respect of claims

1-6

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
A	GB 2162975 A "TECHNOPARK MINE CO" - see abstract	1

Category	Identity of document and relevant passages	Relevant to claim(s)

### Categories of documents

**X:** Document indicating lack of novelty or of inventive step.

**Y:** Document indicating lack of inventive step if combined with one or more other documents of the same category.

**A:** Document indicating technological background and/or state of the art.

**P:** Document published on or after the declared priority date but before the filing date of the present application.

**E:** Patent document published on or after, but with priority date earlier than, the filing date of the present application.

**&:** Member of the same patent family, corresponding document.

**Databases:** The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).